EXHIBIT A

20022331

DELIVERED THIS 03 DAY OF MAR, 20 21
ADAN BALLESTEROS
CONSTABLE, PREC. 2 TRAVIS COUNTY, TEXAS
BY 2045 DEPUTY

IN THE 18TH JUDICIAL CIRCUIT, PETTIS COUNTY, MISSOURI

Judge or Division: ROBERT L. KOFFMAN	**Case Number: 21PT-CC00022**
Plaintiff/Petitioner: MILDRED BALDWIN vs.	Plaintiff's/Petitioner's Attorney/Address: JOHN FRANCIS GARVEY JR 8235 FORSYTH BLVD STE 1100 ST LOUIS, MO 63105
Defendant/Respondent: NATIONAL WESTERN LIFE INSURANCE COMPANY	Court Address: 415 SOUTH OHIO STE 324 SEDALIA, MO 65301
Nature of Suit: CC Other Tort	(Date File Stamp)

Summons for Personal Service Outside the State of Missouri
(Except Attachment Action)

The State of Missouri to: NATIONAL WESTERN LIFE INSURANCE COMPANY
Alias:
ATTN: OFFICER OR DIRECTOR
10801 N. MOPAC EXPWY, BLDG 3
AUSTIN, TX 78759

COURT SEAL OF CIRCUIT COURT OF MISSOURI ***PETTIS COUNTY***

You are summoned to appear before this court and to file your pleading to the petition, copy of which is attached, and to serve a copy of your pleading upon the attorney for the plaintiff/petitioner at the above address all within 30 days after service of this summons upon you, exclusive of the day of service. If you fail to file your pleading, judgment by default will be taken against you for the relief demanded in this action.

February 18, 2021 (Date) SUSAN SADLER by /s/ Cindi Ross (Clerk)

Further Information:

Officer's or Server's Affidavit of Service

I certify that:

1. I am authorized to serve process in civil actions within the state or territory where the above summons was served.
2. My official title is _____ of _____ County, _____ (state).
3. I have served the above summons by: (check one)
   - ☐ delivering a copy of the summons and a copy of the petition to the defendant/respondent.
   - ☐ leaving a copy of the summons and a copy of the petition at the dwelling place or usual abode of the defendant/respondent with _____, a person of the defendant's/respondent's family over the age of 15 years who permanently resides with the defendant/respondent.
   - ☐ (for service on a corporation) delivering a copy of the summons and a copy of the petition to _____ (name) _____ (title).
   - ☐ other: _____.

Served at _____ (address)

in _____ County, _____ (state), on _____ (date) at _____ (time).

_____ Printed Name of Sheriff or Server

_____ Signature of Sheriff or Server

Subscribed and sworn to before me this _____ (day) _____ (month) _____ (year).

I am: (check one)
- ☐ the clerk of the court of which affiant is an officer.
- ☐ the judge of the court of which affiant is an officer.
- ☐ authorized to administer oaths in the state in which the affiant served the above summons. (use for out-of-state officer)
- ☐ authorized to administer oaths. (use for court-appointed server)

(Seal)

_____ Signature and Title

Service Fees

Summons $_____
Non Est $_____
Mileage $_____ (_____ miles @ $ _____ per mile)
Total $_____

See the following page for directions to officer making return on service of summons.

Directions to Officer Making Return on Service of Summons

A copy of the summons and a copy of the motion must be served on each defendant/respondent. If any defendant/respondent refuses to receive the copy of the summons and motion when offered, the return shall be prepared accordingly so as to show the offer of the officer to deliver the summons and motion and the defendant's/respondent's refusal to receive the same.

Service shall be made: (1) On Individual. On an individual, including an infant or incompetent person not having a legally appointed guardian, by delivering a copy of the summons and motion to the individual personally or by leaving a copy of the summons and motion at the individual's dwelling house or usual place of abode with some person of the family over 15 years of age who permanently resides with the defendant/respondent, or by delivering a copy of the summons and petition to an agent authorized by appointment or required by law to receive service of process; (2) On Guardian. On an infant or incompetent person who has a legally appointed guardian, by delivering a copy of the summons and motion to the guardian personally; (3) On Corporation, Partnership or Other Unincorporated Association. On a corporation, partnership or unincorporated association, by delivering a copy of the summons and motion to an officer, partner, or managing or general agent, or by leaving the copies at any business office of the defendant/respondent with the person having charge thereof or by delivering copies to its registered agent or to any other agent authorized by appointment or required by law to receive service of process; (4) On Public or Quasi-Public Corporation or Body. Upon a public, municipal, governmental or quasi-public corporation or body in the case of a county, to the mayor or city clerk or city attorney in the case of a city, to the chief executive officer in the case of any public, municipal, governmental, or quasi-public corporation or body or to any person otherwise lawfully so designated.

Service may be made by an officer or deputy authorized by law to serve process in civil actions within the state or territory where such service is made.

Service may be made in any state or territory of the United States. If served in a territory, substitute the word "territory" for the word "state."

The office making the service must swear an affidavit before the clerk, deputy clerk, or judge of the court of which the person is an officer or other person authorized to administer oaths. This affidavit must state the time, place, and manner of service, the official character of the affiant, and the affiant's authority to serve process in civil actions within the state or territory where service is made.

Service must be made less than 10 days nor more than 30 days from the date the defendant/respondent is to appear in court. The return should be made promptly, and in any event so that it will reach the Missouri court within 30 days after service.

MISSOURI CIRCUIT COURT
18TH JUDICIAL CIRCUIT
(PETTIS COUNTY)

MILDRED BALDWIN, on behalf of herself and others similarly situated,	
Plaintiff,	**CAUSE NO.**
VS.	
	JURY TRIAL DEMANDED
NATIONAL WESTERN LIFE INSURANCE COMPANY, Serve: Officer or Director 10801 N. Mopac Expressway, Blvd. 3 Austin, TX 78759 (Travis County)	
Defendant.	

CLASS ACTION PETITION

Plaintiff Mildred Baldwin ("Plaintiff"), on behalf of herself and the proposed classes defined below, by Turke & Strauss LLP, alleges as follows:

NATURE OF THE ACTION

1. Defendant National Western Life Insurance Company ("Defendant" or "NWL") is a life-insurance company which, according to its website, offers a broad range of life insurance and annuity products and services.

2. On or about August 15, 2020, NWL discovered that an unauthorized person had gained access to NWL's computer systems (the "Data Breach"). The unauthorized person stole 656 gigabytes worth of confidential and protected personally identifiable information ("PII"), which included the PII of NWL's former and current policyholders.

3. Within days of the Data Breach, the unauthorized person began publishing the leaked PII online. In the first of a series of posts, the unauthorized person published a screen shot of what appears to be a file containing Data Breach victims' credit card information. A few days

later, on or about August 23, 2020, the unauthorized person posted screenshots of policyholders' Social Security numbers, dates of birth, full names, dates of death, addresses, policy numbers, and policy termination dates.

4. Instead of notifying victims of the Data Breach promptly, NWL waited almost 4 months—until December 21, 2020—to start notifying policyholders of the Breach.

5. According to NWL, the delay in notifying Data Breach victims was because the company was undergoing an investigation.

6. At best, NWL should have known that its policyholders' PII was being publicly disseminated on the internet. At worst, NWL, upon information or belief, knew the severity of the Data Breach but chose to ignore and downplay the ongoing public disclosure of the Data Breach victims' PII.

7. Plaintiff received a form notification letter dated January 25, 2021 (the "Notice Letter"), nearly five months after the Data Breach. The form letter notified Plaintiff that "On August 15, 2020, NWL discovered a malware incident impacting certain company systems" and that "On December 21, 2020 we confirmed that personal information related to you was included in the impacted data."

8. The Notice Letter did not warn Plaintiff that the unauthorized accessor was publicly disclosing Data Breach victims' PII in a series of online posts. Upon information and belief, NWL was attempting to downplay the Data Breach's impact and severity.

9. Plaintiff and members of the proposed classes are victims of Defendant's negligence and deceptive trade practices. Specifically, Plaintiff and members of the proposed classes trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices in order to prevent the Data Breach that occurred on

August 15, 2020, and when the Data Breach was discovered, Defendant attempted to downplay and minimize the impact of the Breach.

10. Defendant's negligence and deceptive practices caused real and substantial damage to Plaintiff and members of the proposed classes.

11. Plaintiff and members of the proposed classes therefore bring this lawsuit seeking damages and restitution for Defendant's actions.

THE PARTIES

12. Plaintiff Mildred Baldwin is a natural person and citizen of the state of Missouri, residing in Sedalia, Missouri.

13. Defendant NWL is a Colorado corporation that maintains its principal place of business in Austin, Texas. At all relevant times, NWL routinely conducts and does substantial business in Missouri.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action because the amount in controversy and subject matter are within the jurisdictional limits of this Court.

15. This Court has personal jurisdiction over Defendant because Defendant does substantial business in this State. Defendant is registered with the State of Missouri to sell insurance products and at all relevant times to this action, sought and solicited its insurance products in Missouri.

16. Upon information and belief, NWL recruits and trains agents to sell its life insurance products in Missouri.[1]

[1] *See, e.g.*, https://evervest.us/wp-content/uploads/2019/07/National-Western-Product-Training.pdf (last visited February 10, 2021).

17. Venue is proper in Pettis County pursuant to RSMO 508.010(4) in that Plaintiff's injury first occurred in Pettis County. Due to NWL's negligent and/or reckless failure to properly protect and maintain Plaintiff's information, Plaintiff's injuries and damages occurred in Pettis County.

COMMON FACTUAL ALLEGATIONS

18. Plaintiff and members of the proposed classes are current and former policyholders of NWL.

19. As a prerequisite to coverage, NWL requires purchasers of its life insurance policies and annuities to provide NWL with their PII. In its ordinary course of business, NWL maintains policyholders' full names, addresses, dates of birth, dates of death, Social Security numbers, policy numbers, policy termination dates, driver's license information and passport information.

20. NWL informs the purchasers of its life insurance products that NWL collects and maintains policyholders PII through its Customer Privacy Policy (the "Privacy Policy"). NWL makes state and territory-specific Customer Privacy Policies available on its website at https://www.nationalwesternlife.com/PrivacyPolicy (last visited February 12, 2021).

21. The Privacy Policy states that "National Western Life does not disclose nonpublic personal information about you to anyone except as is necessary in order to provide our products or services to you or as required or permitted by law or as authorized by you." The Privacy Policy also states that that NWL "restrict[s] access to nonpublic personal information about you to those employees and agents who need to know that information to provide products or services to you." The Privacy Policy as it relates to Missouri is attached heretoas **Exhibit A.**

22. Plaintiff and members of the proposed classes relied on NWL's representations that their PII would be secure before purchasing life insurance policies form NWL.

23. In purchasing NWL's life insurance policies, Plaintiff and members of the proposed classes relied on NWL to keep their PII confidential and security maintained.

24. At least as of August 15, 2020, NWL discovered that the PII of its former and current policyholders was compromised. Within days, the unauthorized accessor of NWL's computer systems publicly disclosed that it stole 656 gigabytes worth of PII from NWL's computer systems.

25. Upon information and belief, NWL failed to adequately train its employees on even the basic cybersecurity protocols, including:

a. Effective password management and encryption protocols, including, but not limited to, the use of Multi-Factor Authentication for all users;

b. Locking, encrypting and limiting access to computers and files containing sensitive information;

c. Implementing guidelines for maintaining and communicating sensitive data;

d. Protecting sensitive patient information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients; and

e. Providing focused cybersecurity awareness training programs foremployees.

26. NWL's negligent conduct caused the Data Breach. NWL violated its obligation to implement best practices and comply with industry standards concerning computer system security. NWL failed to comply with security standards and allowed its policyholders' PII to be stolen by failing to implement security measures that could have prevented or mitigated the Data Breach.

A. The Data Breach and Notice Letter

27. NWL ultimately admitted to the Data Breach on or about December 21, 2020. In the Notice Letter to Plaintiff (attached hereto as **Exhibit B**) and, upon information and belief, sent to the proposed classes, NWL admitted that:

> On August 15, 2020, NWL discovered a malware incident impacting certain company systems. We immediately launched an investigation, with the assistance of third-party investigators, to determine the nature and scope of this event. The investigation confirmed that certain data had been accessed and/or acquired by an unauthorized actor as a result of this event from August 7 to August 10, 2020. On December 21, 2020 we confirmed that personal information related to you was included in the impacted data.

28. NWL identified only the following actions it undertook to mitigate and remediate the harm caused by the Data Breach in the Notice Letter:

> As part of our ongoing commitment to the security of information, we notified federal law enforcement and we are reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

Ex. B.

29. NWL recognized the substantial and high likelihood that Plaintiff and the proposed classes' PII would be misused, instructing Plaintiff and the proposed classes to:

> Please review the enclosed *Steps You can Take to Protect Your Information*, which contains information on what you can do to better protectagainst possible misuse of your information. We encourage you to remainvigilant against incidents of identify theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

Id. (parenthesis in the original).

30. NWL encouraged its policyholders to contact the three credit-reporting bureaus to either place a "security freeze" or a "fraud alert" on their credit reports.

B. PII is Stolen and Plaintiff Faces Significant Risk of Identity Theft

31. Within days of the Data Breach, Data Breach victims' PII began being posted online.

32. On or about August 18, 2020, Cyble Vision, a digital Risk Management Platform, discovered that the unauthorized accessor of NWL's computer systems posted, on an online ransomware forum, that the accessor has stolen 656 gigabytes of NWL's confidential data. A copy Cyble Vision's reporting is attached hereto as **Exhibit C.**

33. In the online post, the unauthorized accessor shared screenshots of a file that appears to contain credit card information of NWL's policyholders.

34. On or about August 23, 2020, the unauthorized user published another post sharing screenshots of NWL's policyholder's Social Security numbers, dates of birth, full name, dates of death, residence state, policy numbers, and policy termination date. *See* Ex. C.

35. Plaintiff and members of the proposed classes have suffered injury from the misuse of their PII that can be directly traced to Defendant.

36. As a result of NWL's failure to prevent the Data Breach, Plaintiff and the proposed classes have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII;

h. The continued risk to their PII, which remains in the possession of NWL and is subject to further breaches so long as NWL fails to undertake the appropriate measures to protect the PII in their possession.

37. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[2]

38. The value of Plaintiff's and the proposed classes PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

39. It can take victims years to spot identity or PII theft, giving criminals plenty of time to milk that information for cash.

[2] *See* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web*, EXPERIAN, (Dec. 15, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited February 9, 2021).

40. One such example of criminals using PII for profit is the development of "Fullz" packages.[3]

41. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

42. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed classes' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed classes, and it is reasonable for any trier of fact, including this Court or a jury, to find

[3] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014), *available at* https://krebsonsecurity.com/tag/fullz/, (last visited February 10, 2020).

that Plaintiff's and other members of the proposed classes' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

43. NWL disclosed the PII of Plaintiff and members of the proposed classes for criminals to use in the conduct of criminal activity. Specifically, NWL opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed classes to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity fraud), all using the stolen PII.

44. NWL's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and thousands of members of the proposed classes to unscrupulous operators, con artists and outright criminals.

45. NWL's failure to properly notify Plaintiff and members of the proposed classes of the Data Breach exacerbated Plaintiff's and members of the proposed classes' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

46. Upon information and belief, NWL knew the severity of the Data Breach but chose to downplay the Data Breach's impact. In the Notice Letter to Plaintiff and members of the proposed classes, NWL did not disclose that the unauthorized accessor had been publicly disclosing Data Breach victims' PII online since August 2020 and that the unauthorized accessor had the ability to continually do so.

PLAINTIFF'S EXPERIENCE

47. Ms. Baldwin is a resident of and citizen of Missouri. Upon information and belief, Ms. Baldwin purchased a life insurance policy from NWL in 1994. Upon information and belief, the life insurance policy lapsed the same year.

48. As a condition of the life insurance policy purchase, NWL required Ms. Baldwin to provide the company with her PII.

49. Ms. Baldwin provided NWL her PII in order to purchase and receive the benefits of the life insurance policy.

50. On or about January 25, 2021, Ms. Baldwin received the Notice Letter from NWL, which informed her of the Data Breach and that she faced a substantial and significant risk of her PII being misused.

51. The Notice Letter did not inform Ms. Baldwin that the unauthorized accessor of NWL's computer systems had been posting Data Breach victims' PII online since August 2020.

52. As a result of the Data Breach, Ms. Baldwin expends a considerable time and effort monitoring her accounts to protect herself from additional identity theft. Ms. Baldwin fears for her personal financial security and is experiencing feelings of rage and anger, anxiety, sleep disruption, stress, fear, and physical pain. This goes far beyond allegations of mere worry or inconvenience; it is exactly sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

CLASS ALLEGATIONS

53. Plaintiff brings this action pursuant to Missouri Court Rule of Civil Procedure 52.08 on behalf of herself and all members of the proposed class (the "Classes") as defined as:

> **National Class:** All persons in the United States who are current and former policy holders of Defendant and who were mailed and received the Notice Letter.
>
> **Missouri Class:** All persons in Missouri who are current and former policy holders of Defendant and who were mailed and received the Notice Letter.

54. The following people are excluded from the Classes: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

55. Plaintiff and members of the Classes satisfy the numerosity, commonality, typicality, adequacy, and predominance prerequisites for suing as representative parties pursuant to Rule 52.08(a).

56. **Numerosity:** The exact number of members of the Classes is unknown but, upon information and belief, it is estimated to be number in the thousands at this time, and individual joinder in this case is impracticable. Members of the Classes can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies.

57. **Typicality**: Plaintiff's claims are typical of the claims of other members of the Classes in that Plaintiff, and the members of the Classes sustained damages arising out of

Defendant's Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiff and members of the Classes sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

58. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Classes and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Classes. Plaintiff has no interests that conflict with, or are antagonistic to those of, the Classes, and Defendant has no defenses unique to Plaintiff.

59. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include, but are not necessarily limited to the following:

a. whether Defendant violated the laws asserted herein, including statutory privacy laws;

b. whether Defendant had a duty to use reasonable care to safeguard Plaintiff's and members of the Classes' PII;

c. whether Defendant breached the duty to use reasonable care to safeguard members of the Classes' PII;

d. whether Defendant breached its contractual promises to safeguard Plaintiff's and members of the Classes' PII;

e. whether Defendant knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing sensitive PII;

f. whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff's and members of the Classes' PII from unauthorized release and disclosure;

g. whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiff's and members of the Classes' PII from unauthorized release and disclosure;

h. whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

i. whether Defendant's delay in informing Plaintiff and members of the Classes of the Data Breach was unreasonable;

j. whether Defendant's method of informing Plaintiff and other members of the Classes of the Data Breach was unreasonable;

k. whether Defendant's conduct was likely to deceive the public;

l. whether Defendant is liable for negligence or gross negligence;

m. whether Defendant's conduct, practices, statements, and representations about the Data Breach of the PII violated applicable state laws;

n. whether Plaintiff and members of the Classes were injured as a proximate cause or result of the Data Breach;

o. whether Plaintiff and members of the Classes were damaged as a proximate cause or result of Defendant's breach of its contract with Plaintiff and members of the Classes;

p. whether Defendant's practices and representations related to the Data Breach breached implied warranties;

q. what the proper measure of damages is; and

r. whether Plaintiff and members of the Classes are entitled to restitutionary, injunctive, declaratory, or other relief.

60. **Superiority:** This cause is also appropriate for class certification becauseclass proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Classes will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Classes to obtain effective relief from Defendant's misconduct. Even if members of the Classes could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions ensured.

61. A class action is therefore superior to induvial litigation because:

a. the amount of damages available to an individual plaintiff is insufficient to make litigation addressing Defendant's conduct economically feasible in the absence of the class action procedural device;

b. individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

Count I
Negligence
(On Behalf of Plaintiff, the National Class, and the Missouri Class)

62. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

63. Plaintiff and members of the Classes entrusted their PII to Defendant. Defendant owed to Plaintiff and other members of the Classes a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

64. Defendant owed a duty of care to Plaintiff and members of the Classes because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Classes' PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the manner in which the PII was stored, used, and exchanged, and those in its employee who were responsible for making that happen.

65. Defendant owed to Plaintiff and members of the Classes a duty to notify them within a reasonable time frame of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Classes the scope, nature, and occurrence of the Data Breach. This duty is required and necessary in order for Plaintiff and members of the Classes to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

66. Defendant owed these duties to Plaintiff and members of the Classes because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Classes' personal information and PII for insurance products purposes. Plaintiff and members of the Classes were required to provide their personal information and PII to Defendant in order to receive insurance services from Defendant, and Defendant retained that information.

67. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

68. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Classes, and the importance of exercising reasonable care in handling it.

69. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal

information and PII of Plaintiff and members of the Classes which actually and proximately caused the Data Breach and Plaintiff's and members of the Classes' injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Classes, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Classes' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Classes have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

70. Defendant's breach of its common law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and members of the Classes actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Missouri Class)

71. Plaintiff and the Missouri Class members incorporate the above allegations as if fully set forth herein.

72. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Missouri Class members' PII.

73. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, policyholders' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Missouri Class members' sensitive PII.

74. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect its policyholders' PII and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to policyholders in the event of a breach, which ultimately came to pass.

75. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Missouri Class members.

76. Defendant had a duty to Plaintiff and the Missouri Class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Missouri Classes' PII.

77. Defendant breached its respective duties to Plaintiff and members of the Missouri Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Missouri Class members' PII.

78. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

79. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Missouri Class, Plaintiff and the members of the Missouri Class would not have been injured.

80. The injury and harm suffered by Plaintiff and the Missouri Class members were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Missouri Class to suffer the foreseeable harms associated with the exposure of their PII.

81. Had Plaintiff and members of the Missouri Class known that Defendant did not adequately protect policyholders' PII, Plaintiff and members of the Missouri Class would not have entrusted Defendant with their PII.

82. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Missouri Class members have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the treatment Plaintiff and the Missouri Class members paid for that they would not have received had they known of Defendant's careless approach to cyber security; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

83. Defendant publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff and the Missouri Class members by disclosing and exposing Plaintiff's and the Missouri Class members' PII to enough people that it is reasonably likely those facts will become known to the public at large, including, without limitation, on the dark web and elsewhere.

84. The disclosure of policyholders' full names, addresses, dates of birth, dates of death, Social Security numbers, policy numbers, policy termination dates, driver's license information, and passport information is particularly harmful and would be offensive to a reasonable person of ordinary sensibilities.

85. Defendant has a special relationship with Plaintiff and the Missouri Class members and Defendant's disclosure of PII is certain to embarrass them and offend their dignity. Defendant should appreciate that the cyber-criminals who stole the PII would further sell and disclose the PII as they are doing. That the original disclosure is devastating to the Plaintiff and the Missouri Class members, even though it originally may have only been disclosed to one person or a limited number of cyber-criminals, does not render it any less a disclosure to the public-at-large.

86. The tort of public disclosure of private facts is recognized inMissouri. *See Sullivan v. Pulitzer Broad. Co.*, 709 S.W.2d 475 (Mo. 1986). Plaintiff's and the Missouri Classmembers' PII was publicly disclosed by Defendant in the Data Breach with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendant knew or should have known that Plaintiff's and the Missouri Class members' PII is not a matter of legitimate public concern. As a direct and proximate result of Defendant's conduct, Plaintiff and Missouri Class members have been injured and are entitled to damages.

COUNT II
Breach of Express/Implied Contractual Duty
(On Behalf of Plaintiff, the National Class, and the Missouri Class)

87. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

88. Defendant offered to provide life insurance to Plaintiff and members of the Classes in exchange for payment.

89. Defendant also required Plaintiff and the members of the Classes to provide Defendant with their PII in order to purchase life insurance from Defendant.

90. In turn, and through its Privacy Policy, Defendant agreed it would not disclose PII it collects from customers to unauthorized persons. Defendant also promised to maintain safeguards to protect customers' PII.

91. Plaintiff and the members of the Classes accepted Defendant's offer by providing PII to Defendant in applying for life insurance related products and services and then by paying for and receiving the same.

92. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Classes with prompt and adequate notice of any and all unauthorized access and/or theft of their PII.

93. Plaintiff and the members of the Classes would not have entrusted their PII to Defendant in the absence of such agreement with Defendant.

94. Defendant materially breached the contract(s) it had entered with Plaintiff and members of the Classes by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and members of the Classes by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Classes' PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

95. The damages sustained by Plaintiff and members of the Classes as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

96. Plaintiff and members of the Classes have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

97. The convent of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

98. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

99. Defendant failed to advise Plaintiff and members of the Classes of the Data Breach promptly and sufficiently.

100. In these and other ways, Defendant violated its duty of good faith and fair dealing.

101. Plaintiff and members of the Classes have sustained damages as a result of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff, the National Class, and Missouri Class)

102. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

103. This claim is plead in the alternative to the breach of implied contractual duty claim.

104. Plaintiff and members of the Classes conferred a monetary benefit upon Defendant in the form of monies paid for life insurance.

105. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Classes. Defendant also benefited from the receipt of Plaintiff's and members of the Classes' PII, as this was used to facilitate payment and insurance claims.

106. As a result of Defendant's conduct, Plaintiff and members of the Classes suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff and members of the Classes paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

107. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and members of the Classes because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for

itself that Plaintiff and members of the Classes paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

108. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Classes all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT IV
Violation of the Missouri Merchandising Practices Act (MMPA)
Mo. Stat. § 407.010, *et seq.*
(On Behalf of Plaintiff and the Missouri Class)

109. Plaintiff and the Missouri Class members incorporate the above allegations as if fully set forth herein.

110. Plaintiff and the Missouri Class members are "consumers" as that term is defined in the Missouri Merchandising Practices Act (MMPA).

54. Defendant was engaged in the sale of a "merchandise in trade of commerce" as defined under the MMPA.

55. Defendant's business of providing life insurance coverage services was primarily for "personal," "family," or "household" purposes.

56. Plaintiff and the Missouri Class members purchased Defendant's services when Plaintiff and the Missouri Class members paid Defendant for insurance coverage.

57. As part of that transaction, Defendant required Plaintiff and the Missouri Class members to provide Defendant with the patients' names, dates of birth, Social Security numbers, and personal financial information.

58. As recounted above, the value of Plaintiff's and the Missouri Class members' PII is considerable. Hence, Plaintiff's and the Missouri Class members would not have provided

Defendant with their PII absent representation and assurances from Defendant that the PII would be secure.

59. Defendant failed to reveal material facts in connection with the sale and advertisement of its services in violation of the MMPA, including, but not limited to, the following:

a. Failing to maintain sufficient data security to keep Plaintiff's and the Missouri Class members; sensitive PII secure.

b. Misrepresenting material facts to the class, in connection with the sale of goods and services by representing that Defendant would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and the Missouri Class members' PII from unauthorized disclosure, release, and theft.

c. Misrepresenting material facts to Plaintiff and the Missouri Class members in connection with sale of goods and services by representing that Defendant did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and the Missouri Class members' PII.

d. Failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff and the Missouri Class members' PII from further unauthorized disclosure, release, data breaches, and theft.

60. In addition, Defendant's failure to disclose that its computer systems were not well-protected, and that Plaintiff's and the Missouri Class members' PII was vulnerable and susceptible to intrusion while it was entrusted to Defendant, constitutes deceptive and/or unfair acts or practices because Defendant knew such facts would (a) be unknown to and not easily discoverable by Plaintiff and the Missouri Class members; and (b) defeat Plaintiff's and the Missouri Class members' ordinary, foreseeable, and reasonable expectations concerning the security of their PII.

61. Defendant also engaged in unfair acts and practices by failing to maintain the privacy and security of the Missouri Class members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

62. Defendant's wrongful practices occurred in the course of trade or commerce.

63. As a direct and proximate result of Defendant's conduct, Plaintiff and the Missouri Class members have suffered harm, including, but not limited to, loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the services rendered at Defendant; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from stolen use of personal information, entitling them to damages in an amount to be proven at trial.

64. Plaintiff and the Missouri Class members seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the MMPA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed Classes, requests that the Court:

A. Certify this case as a class action on behalf of the Classes defined above, appoint Plaintiff Mildred Baldwin as the Class representative, and appoint the undersigned as Class counsel;

B. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Classes;

C. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Classes;

D. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PII;

E. Enter an award in favor of Plaintiff and the Classes that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

F. Award restitution and damages to Plaintiff and the Classes in an amount to be determined at trial;

G. Enter an award of attorneys' fees and costs, as allowed by law;

H. Enter an award of prejudgment and post-judgment interest, as provided by law;

I. Grant Plaintiff and the Classes leave to amend this petition to conform to the evidence produced at trial; and

J. Grant such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demand a trial by jury on all issues so triable.

Dated: February 16, 2021.

Respectfully submitted,

CAREY DANIS & LOWE

By: */s/John F. Garvey*
John F. Garvey #35879
8235 Forsyth, Ste. 1100
St. Louis, MO 63105
Tel: (314) 725-7700
jgarvey@careydanis.com

Lynn A. Toops*
Lisa M. La Fornara*
COHEN & MALAD, LLP
One Indiana Square
Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481
ltoops@cohenandmalad.com
llafornara@cohenandmalad.com

Samuel J. Strauss*
TURKE & STRAUSS LLP
613 Williamson Street Suite 201
Madison, WI 53703
Tel: (608) 237-1775
Sam@turkestrauss.com

J. Gerard Stranch, IV*
Peter J. Jannace*
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gerards@bsjfirm.com
peterj@bsjfirm.com

*Motion for admission to be filed

Counsel for Plaintiff and the Proposed Class

Certificate of Service

The undersigned hereby certifies that the foregoing Class Action Petition has been filed by using the court's electronic case filing system on this 16th day of February, 2021.

/s/John F. Garvey

MISSOURI CIRCUIT COURT
18TH JUDICIAL CIRCUIT
(PETTIS COUNTY)

MILDRED BALDWIN, on behalf of herself and others similarly situated,	)	
Plaintiff,	)	**CAUSE NO. 21PT-CC00022**
VS.	)	
NATIONAL WESTERN LIFE INSURANCE COMPANY,	)	
Defendant.	)	

CERTIFICATE OF SERVICE

The undersigned hereby certifies that Plaintiff's First Set of Eleven (11) Interrogatories Directed to Defendant National Western Life Insurance Company and Plaintiff's First Set of Nineteen (19) Requests for Production of Documents and Things Directed to Defendant National Western Life Insurance Company have been provided to the Constable of Travis County, Texas for service upon Defendant at the below stated address simultaneously with service of the Summons and Class Action Petition on this 24th day of February, 2021:

National Western Life Insurance Company
Attn: Officer of Director
10801 N. Mopac Expressway, Blvd. 3
Austin, TX 78759
Defendant

Respectfully submitted,

/s/John F. Garvey
John F. Garvey #35879
CAREY DANIS & LOWE
8235 Forsyth Blvd., Ste. 1100
St. Louis, MO 63105
Tel: (314) 725-7700
Fax: (314) 678-3401
jgarvey@careydanis.com

Lynn A. Toops
Lisa M. La Fornara*
COHEN & MALAD, LLP
One Indiana Square
Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481
ltoops@cohenandmalad.com
llafornara@cohenandmalad.com

Samuel Strauss*
Austin Doan*
TURKE & STRAUSS, LLP
613 Williamson Street Suite 201
Madison, WI 53703
Ph: (608) 237-1775
Sam@turkestrauss.com
AustinD@turkestrauss.com

J. Gerard Stranch, IV*
Peter J. Jannace*
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gerards@bsjfirm.com
peterj@bsjfirm.com

*Motion for admission to be filed

Counsel for Plaintiff and the Proposed Class

CERTIFICATE OF FILING

I hereby certify that the foregoing Certificate of Service has been filed by using the Court's electronic case filing system on this 24th day of February, 2021.

/s/John F. Garvey
John F. Garvey- 35879

MISSOURI CIRCUIT COURT
18TH JUDICIAL CIRCUIT
(PETTIS COUNTY)

MILDRED BALDWIN, on behalf of herself and others similarly situated,	)	
Plaintiff,	)	**CAUSE NO. 21PT-CC00022**
VS.	)	
NATIONAL WESTERN LIFE INSURANCE COMPANY,	)	
Defendant.	)	

PLAINTIFF'S FIRST SET OF ELEVEN (11) INTERROGATORIES DIRECTED TO DEFENDANT NATIONAL WESTERN LIFE INSURANCE COMPANY

Pursuant to Rules 56.01 and 57.01 of the Missouri Rules of Civil Procedure, Plaintiff hereby requests that Defendant National Western Life Insurance Company produce answers under oath to the eleven (11) Interrogatories contained herein in accordance with the instructions and definitions below within forty-five (45) days after the date upon which it has been served with process in the above captioned action. The following Interrogatories are to be considered continuing in nature and must be supplemented or amended to the extent required by the Missouri Rules of Civil Procedure.

DEFINITIONS

As used herein the following terms have the following meanings:

(a) "You," or "Your" refers to National Western Life Insurance Company, and any present or former officers, directors, agents, employees, members, representatives, consultants, attorneys, or other persons acting or purporting to act on behalf of such person or entity.

(b) "Affected person" means any individual whom National Western Life Insurance Company notified of the Data Breach.

(c) "Document" includes all books, documents, communications, information, or tangible things within the scope of Missouri Rules of Civil Procedure 56.01 and 58.01, whether in Your direct or indirect custody or control, including ESI and all versions and drafts of said documents.

(d) "Data Breach" refers to the incident that occurred between on or about August 7 and August 10, 2020 and that National Western Life Insurance Company began notifying Affected persons about on or around January 25, 2021.

(e) "Personally Identifiable Information" or "PII" is an individual's name, date of birth, Social Security Number, policy numbers of current or former life insurance of annuity policies, and any other sensitive information entrusted to National Western Life Insurance Company that was potentially compromised in the Data Breach.

INSTRUCTIONS

(f) Unless otherwise stated, the relevant time period for these requests is August 7, 2015 through the present.

(g) These requests are continuing in nature and require supplemental answer, response and production.

INTERROGATORIES

1. Describe with particularity all of Your policies and procedures regarding the collection and retention of PII from insureds, their beneficiaries and any other Affected persons, including, but not limited to, the specific data collected and retained, the length of time that data is retained, and any procedures in place to ensure that these policies and procedures were and are being followed.

ANSWER:

2. Describe with particularity all of Your policies and procedures regarding the safeguarding and protection of PII including, but not limited to, Your costs associated therewith, as well as any procedures, practices, and training in place to ensure that these policies and procedures were and are being followed.

ANSWER:

3. Describe any representations You made to Your current and former insureds, their beneficiaries and any other Affected persons regarding the protection and security of PII stored in Your systems, including but not limited to compliance with any state or federal privacy or information security laws or regulations.

ANSWER:

4. Identify and describe any and all remedial steps You took during or following the Data Breach.

ANSWER:

5. Identify and describe any changes to the structure of Your policies, procedures, and

practices for security of patient information and Your communications and training regarding the same that were recommended to You before August 7, 2020, including but not limited to the nature of those recommended changes, the identity of the individuals and/or corporate entities that recommended the changes, whether the changes were actually made, the reasons You made or disregarded the changes, and the individuals and/or corporate entities involved in approving, denying, and implementing the recommended changes.

ANSWER:

6. Identify and describe all changes You made or plan to make to Your policies, procedures, and practices for security of insureds, their beneficiaries and any other Affected persons' information and Your communications and training regarding the same during or after the Data Breach, including but not limited to the nature of those changes, the actual or probable effect of those changes, and the individuals and/or corporate entities involved in approving, denying, and implementing those changes.

ANSWER:

7. For the Data Breach, describe:

(a) The date and time Affected persons' PII stored on Your systems was first made accessible to unauthorized parties;

(b) The date and time when You first learned that the information stored on Your systems had been compromised by unauthorized parties;

(c) The date on which You first notified Your current and former insureds, their beneficiaries and any other Affected persons, government entities, and/or the public that information on Your systems had been compromised; and

(d) The method through which You notified Your current and former insureds, their beneficiaries and any other Affected persons, government entities, and/or the public that information on Your systems had been compromised.

ANSWER:

8. Identify and describe the process through which You decided when and how to notify Your current and former insureds, their beneficiaries and any other Affected persons, government entities, and/or the general public of the Data Breach, including, but not limited to, the corporate entities or individuals involved in that decision and the considerations evaluated.

ANSWER:

9. For each individual to whom you sent (or caused to be sent) notification of the Data Breach, identify the individual by a unique identifier and identify their state of residence and the types of their PII that You determined potentially were compromised in the Data Breach.

ANSWER:

Individual Identifier	State of Residence	PII Potentially Compromised

10. Describe with particularity the extent to which any information that was stored on Your systems and was improperly compromised during the Data Breach has been misused by unauthorized individuals, including but not limited to instances of identity theft, fraud, or the discovery of this information for sale on the dark web.

ANSWER:

11. Identify and describe any remedial products or services you made available to individuals whose PII was stored on your systems and compromised during the Data Breach, including but not limited to the availability of free credit monitoring services and the number and proportion of affected persons who claimed the offered remedial products or services, including, but not limited to, enrollment in any offered credit monitoring services.

ANSWER:

Dated: February 24, 2021

Respectfully submitted,

/s/John F. Garvey

John F. Garvey #35879
CAREY DANIS & LOWE
8235 Forsyth Blvd., Ste. 1100
St. Louis, MO 63105
Tel: (314) 725-7700
Fax: (314) 678-3401
jgarvey@careydanis.com

Lynn A. Toops
Lisa M. La Fornara*
COHEN & MALAD, LLP
One Indiana Square
Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481

ltoops@cohenandmalad.com
llafornara@cohenandmalad.com

Samuel Strauss*
Austin Doan*
TURKE & STRAUSS, LLP
613 Williamson Street Suite 201
Madison, WI 53703
Ph: (608) 237-1775
Sam@turkestrauss.com
AustinD@turkestrauss.com

J. Gerard Stranch, IV*
Peter J. Jannace*
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gerards@bsjfirm.com
peterj@bsjfirm.com

*Motion for admission to be filed

Counsel for Plaintiff and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Interrogatories were provide to the Constable of Travis County for service along with and at the time of service of the Class Action Petition in this matter on this 24th day of February, 2021, for service upon Defendant at the following address:

National Western Life Insurance Company
Attn: Officer of Director
10801 N. Mopac Expressway, Blvd. 3
Austin, TX 78759
Defendant

/s/John F. Garvey
John F. Garvey- 35879
CAREY DANIS & LOWE
8235 Forsyth Blvd., Ste. 1100
St. Louis, MO63105

MISSOURI CIRCUIT COURT
18TH JUDICIAL CIRCUIT
(PETTIS COUNTY)

MILDRED BALDWIN, on behalf of herself and others similarly situated,	)	
Plaintiff,	)	**CAUSE NO. 21PT-CC00022**
VS.	)	
NATIONAL WESTERN LIFE INSURANCE COMPANY,	)	
Defendant.	)	

PLAINTIFF'S FIRST SET OF NINETEEN (19) REQUESTS FOR PRODUCTION OF DOCUMENTS AND THINGS DIRECTED TO DEFENDANT NATIONAL WESTERN LIFE INSURANCE COMPANY

Pursuant to Rules 56.01 and 58.01 of the Missouri Rules of Civil Procedure, Plaintiff hereby requests that Defendant National Western Life Insurance Company produce and permit the inspection and copying of the following documents and things in accordance with the instructions and definitions below within forty-five (45) days after the date upon which it has been served with process in the above captioned action. The following Requests for Production of Documents and Things are to be considered continuing in nature and must be supplemented or amended to the extent required by the Missouri Rules of Civil Procedure.

DEFINITIONS

As used herein the following terms have the following meanings:

(a) "You," or "Your" refers to National Western Life Insurance Company, and any present or former officers, directors, agents, employees, members, representatives, consultants, attorneys, or other persons acting or purporting to act on behalf of such person or entity.

(b) "Affected person" means any individual whom National Western Life Insurance Company notified of the Data Breach.

(c) "Document" includes all books, documents, communications, information, or tangible things within the scope of Missouri Rules of Civil Procedure 56.01 and 58.01, whether in Your direct or indirect custody or control, including ESI and all versions and drafts of said documents.

(d) "Data Breach" refers to the incident that occurred between on or about August 7 and August 10, 2020 and that National Western Life Insurance Company began notifying Affected persons about on or around January 25, 2021.

(e) "Personally Identifiable Information" or "PII" is an individual's name, date of birth, Social Security Number, policy numbers of current or former life insurance of annuity policies, and any other sensitive information entrusted to National Western Life Insurance Company that was potentially compromised in the Data Breach.

INSTRUCTIONS

(f) Unless otherwise stated, the relevant time period for these requests is August 7, 2015 through the present.

(g) These requests are continuing in nature and require supplemental answer, response and production.

(h) These document requests call for the production of all responsive documents in Your possession, custody, or control without regard to the physical location of such documents. If any part of a document is responsive to any request, the whole document should be produced.

(i) In producing documents and other materials, You are requested to furnish all documents or things in Your possession, custody, or control, regardless of whether such documents or

materials are possessed directly by You or Your agents, representatives, or by Your attorneys or their agents, employees, representatives or investigators.

(j) Documents shall be produced in such fashion as to identify the department, branch, or office in whose possession they were located and, where applicable, the natural person in whose possession they were found and the business address of each document's custodian(s).

(k) Unless words or terms have been given a specific definition herein, each word or term used shall be given its usual and customary dictionary definition except where such words have a specific custom and usage definition in Your trade or industry, in which case they shall be interpreted in accordance with such usual custom and usage definition of which You are aware.

(l) In construing the inquiry and request herein: (a) the singular shall include the plural and the plural shall include the singular; (b) a masculine, feminine, or neuter pronoun shall not exclude the other genders; (c) the terms "any" and "all" shall be understood to mean "any and all"; and (d) the words "and" and "or" shall be read in the conjunctive or disjunctive or both, as the case may be, all to the end that the interpretation applied results in the more expansive production.

(m) Where a document request refers to a specific time period, the request shall encompass all documents concerning events and circumstances during that time period, even if such documents were dated, prepared, generated, received, or reviewed prior to or after that period.

REQUESTS FOR PRODUCTION OF DOCUMENTS

1. All documents and communications concerning Your policies and procedures regarding the collection and retention of PII from insureds, their beneficiaries and any other Affected persons, including, but not limited to, any procedures in place to ensure that these policies and procedures were and are being followed.

2. All documents and communications concerning Your policies and procedures regarding the safeguarding and protection of PII including, but not limited to, Your costs associated therewith, as well as any procedures, practices, and training in place to ensure that these policies and procedures were and are being followed during the relevant period.

3. All documents concerning any representations You made to Your current and former insureds, their beneficiaries and any other Affected persons regarding the protection and security of PII stored in Your systems, including, but not limited to, compliance with any state or federal privacy or information security laws or regulations.

4. All documents concerning any remedial steps You took during or following the Data Breach.

5. All documents concerning communications between You and any governmental entities that relate to Your policies, procedures, protocols or practices for safeguarding and protecting PII or the Data Breach.

6. All documents regarding Your compliance or noncompliance with any applicable data security guidelines or standards.

7. All documents related to Your policies and procedures to prevent, detect, contain, or remediate security incidents, such as unauthorized access to or disclosure of PII, as well as evidence of compliance or non-compliance with those policies and procedures.

8. All assessments or analyses regarding the potential risks or vulnerabilities to the confidentiality, integrity, and availability of PII in Your systems as well as any decisions or efforts to address or remediate any identified risks.

9. All documents related to Your security awareness and training programs for members of Your workforce, including, but not limited to, names and titles of individuals conducting trainings, training manuals, course materials, topics covered, agendas, notes, and presentations.

10. All documents related to enforcement of Your information security policies and procedures, including records of sanctions for noncompliance with those policies and procedures.

11. Documents sufficient to show the extent to which Your workforce members had completed and were and are up to date with the requirements of Your security awareness and training programs, including, but not limited to, attendance records.

12. All of Your policies and procedures for encryption and decryption of PII and evidence that these policies and procedures were and are being followed.

13. Documents sufficient to show how You identified that the Data Breach occurred, including, but not limited to, how You determined that the security of insureds, their beneficiaries and any other Affected persons' data was compromised, what data was compromised, the dates on which You became aware of the unauthorized access, why the unauthorized access occurred, and any cybersecurity measures or precautions You have implemented in response to the Data Breach.

14. All reports or other documents created to document the Data Breach and its consequences or Your response to the Data Breach, including, but not limited to, the cause of the Data Breach, the information compromised during the Data Breach, the number of affected persons, remedial measures taken, changes implemented and details regarding such measures and changes such as when the changes took place or will take place, and who implemented or will implement the changes.

15. All documents with information regarding the number of individuals whose PII was improperly compromised during the Data Breach, including the age and residency of those individuals.

16. All documents detailing any recommendations made or actions taken to notify affected persons, government entities, or the public of the Data Breach before January 25, 2021, including, but not limited to, the date on which those recommendations or attempts were made and the reasons why notification to affected persons, government entities, or the public was delayed.

17. All documents with information regarding the decision to offer credit monitoring, the level of credit monitoring to offer, the company to use and any other remedial measures or compensation considered or offered as a result of the Data Breach.

18. All documents related to reports of suspicious credit, identify theft, or fraudulent activity that You or Your agent(s) received from any affected person after Your announcement of the Data Breach and all documents related to tracking and recording those reports.

19. All documents memorializing or otherwise pertaining to any express or implied contracts You entered into with Affected persons, including Plaintiff.

Dated: February 24, 2021

Respectfully submitted,

/s/John F. Garvey

John F. Garvey #35879
CAREY DANIS & LOWE
8235 Forsyth Blvd., Ste. 1100
St. Louis, MO 63105
Tel: (314) 725-7700
Fax: (314) 678-3401
jgarvey@careydanis.com

Lynn A. Toops
Lisa M. La Fornara*
COHEN & MALAD, LLP
One Indiana Square
Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481
ltoops@cohenandmalad.com
llafornara@cohenandmalad.com

Samuel Strauss*
Austin Doan*
TURKE & STRAUSS, LLP
613 Williamson Street Suite 201
Madison, WI 53703
Ph: (608) 237-1775
Sam@turkestrauss.com
AustinD@turkestrauss.com

J. Gerard Stranch, IV*
Peter J. Jannace*
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gerards@bsjfirm.com
peterj@bsjfirm.com

*Motion for admission to be filed

Counsel for Plaintiff and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Requests for Production were provide to the Constable of Travis County for service along with and at the time of service of the Class Action Petition in this matter on this 24th day of February, 2021, for service upon Defendant at the following address:

National Western Life Insurance Company
Attn: Officer of Director
10801 N. Mopac Expressway, Blvd. 3
Austin, TX 78759
Defendant

/s/John F. Garvey
John F. Garvey- 35879